УДК 004

Д. Сіньковський, О. Шевченко
(Тернопільський національний технічний університет імені Івана Пулюя)

ШКІДЛИВІ ПРОГРАМИ: ПОНЯТТЯ, ОЗНАКИ, КЛАСИФІКАЦІЯ

Шкідливі програми (Malware – скорочення від «malicious software») – будь-яке програмне забезпечення, спеціально створене для того, щоб завдавати шкоди комп'ютеру, серверу або комп'ютерній мережі, даним незалежно від того, чи є воно вірусом, трояном, мережевим черв'яком і т. д.

Комп'ютерний вірус – різновид комп'ютерної програми, відмінною рисою якої є здатність до розмноження (самореплікації). Вірус може пошкоджувати або повністю знищувати дані на комп'ютері жертви, від імені якого він був запущений.

Поліморфні віруси являють собою певні шкідливі програмні продукти, які після чергового «зараження» ПК жертви утворює свій новий алгоритм, тобто повністю перевтілюється в «нову версію» самого себе ж. Тому даний вид через це свого властивості отримало таке найменування, запозичене з хімічної термінології, і тому даний вид вірусів став дуже важким для виявлення для багатьох антивірусних систем і програмних продуктів. Що б ефективно боротися з такими вірусами у антивірусних засобів повинні бути деякі емулятори та спеціальні алгоритми, написані спеціально під ці віруси і обмежують їх дії.

Хороші і свіжі віруси, які не визначаються антивірусами і здатні обходить системи превентивного контролю (IDS / NIDS / IPS) вартують дуже дорого і спрямовані на крадіжку виключно корпоративної (таємної) комерційної інформації. Інші віруси пишуться в основному ентузіастами, метою яких також є нажива, але, в більшості випадків таке шкідливе ПЗ несе більше руйнівний характер, ніж комерційний, і за умови наявності в системі адекватного адміністратора хорошої кваліфікації можна захиститься від будь-яких вірусів. Адміністратор може бути тільки один і якщо до системи має доступ відразу кілька адміністраторів, то система заздалегідь вважається скомпрометованої!

Історично вірусом називається будь-яка програма, що заражає виконувані або об'єктні файли. Програму, що відтворює себе без відома користувача, також можна віднести до вірусів. Найчастіше вірус поміщає своє тіло в програмному файлі так, щоб він активізувався при кожному запуску програми. Крім того, віруси можуть вражати завантажувальний сектор жорсткого або іншого диска, який поміщається в дисковод зараженого комп'ютера. Перенесення свого тіла на жорсткі диски є для вірусу гарантією того, що він буде запущений при кожному включенні системи. Нижче мова піде про деякі інші способи поширення вірусів.